报业集团网络安全等级保护建设实践与思考

摘　要：文章以网络系统安全等级测评建设要点为立足点，阐述了测评的重要性，详细对网络安全体系的建设要点和日常问题进行了分析，为报业集团技术人员提供安全等级测评建设提供参考

关键词：信息安全体系建设；网络系统安全等级测评
中图分类号：TP393　　文献标识码：A
文章编号：1671-0134（2019）11-126-03　　DOI：10.19483/j.cnki.11-4653/n.2019.11.034

文 / 张亚锋

引言

随着媒体融合不断深入，新媒体业务在报业集团不断壮大，应用系统逐步由原来的采编出版系统转变为全媒体出版系统，由原来内网系统转变为外网系统。近年来，由于新闻网站的权重在重点搜索引擎中占比越来越高，也成为黑客入侵的重点对象。境外博彩业通过不同的形式围攻新闻网站，国内多数新闻网站曾经被入侵，网络安全形势非常严峻。如何保障网络系统安全？网络安全等级保护可以全面保障网络系统的安全稳定运行。

1. 定义测评对象

报业集团现在主要业务系统有新闻采编系统、新媒体制作发布系统、报道指挥系统、媒资系统、经营管理系统、办公系统、互联网邮件及中央厨房等信息系统。这些业务系统都是互联网应用系统，主要威胁有数据越权访问、信息泄漏、非法访问、病毒、木马、APT，自身的安全控制执行力度不够、策略失效、业务漏洞等极易引发网络安全风险。信息系统的等级保护级别，需要从信息系统建设开始就进行规划，同时在单位整体信息化规划时将整互联互通的地方做好边缘隔离，同时共用部分需要按等级保护级别的要求取最高级别。

一般省级报业集团有 10 个左右的三级系统需要进行等级保护测评。近几年报业集团的经营压力较大，网络安全硬件投入又较大，在等级保护测评时，如何能够又省钱又能全面保障安全呢？有些报业集团选择单位的关键基础信息设施进行测评，其它系统没有进行测评，有的甚至只选择一个系统进行测评。也有些报业集团将所有系统作为一个系统来测评，把不同功能作为子系统来进行测评，这样，只需要系统功能描述上对整体功能进行全面说明，同时定好不同子系统之间的边界，确保整个系统全面参加测评，这样可以节省一大笔测评费用。

2. 信息安全体系建设

在等级保护实施过程中，安全管理系统的建设是保障网络系统的基础，是否能够建立全方位的安全管理体系是等级保护实施工作的重点。一个完整的安全管理系统(如图)包括: 安全管理机构、技术管理和安全运维管理，下面开始详细介绍安全管理系统应该包括的内容。

<table>
<tr><th colspan="6">信息安全体系</th></tr>
<tr><td>安全工作管理</td><td colspan="2">管理机构</td><td colspan="2">人员安全</td><td>制度标准</td></tr>
<tr><td>技术管理</td><td>物理</td><td>网络</td><td>主机</td><td>应用</td><td>数据</td></tr>
<tr><td>安全运维管理</td><td colspan="2">系统安全建设</td><td colspan="3">系统安全运维</td></tr>
<tr><td>安全保护对象</td><td>安全计算环境</td><td colspan="2">安全区域边界</td><td colspan="2">安全网络通信</td></tr>
</table>

安全管理机构是管理网络系统的最高领导权力机构，最高领导一般由单位主管领导担任或授权担任，根据情况成立安全管理委员会或安全管理领导小组。安全管理机构设置主管、专职安全管理员，在人员配置上设立三员管理，关键岗位应由多人共同管理。明确审批事项和审批流程，重要事项包括：系统变更、重要操作、物理访问、系统接入、重要活动，建立逐级审批制度和定期审查审批制度。设立日常运行、系统漏洞、数据备份等日常运行事项，同时将日常事项制作成表格。设立全面检查事项，如策略与配置的一致性检查，安全措施的有效性检查，对重大事项应该编写成报告进行总结。

在安全管理人员管理方面，需对安全管理人员进行背景审查、技能考核、签保密协议、签订关键岗位人员协议；人员离岗应及时终止权限，并要求签订离职保密协议。在岗人员需进行安全意识教育和岗位技能培训，

告知安全责任与惩戒措施；不同岗位制定不同培训计划；定期对不同岗位人员进行技能考核。对外部人员访问受控区域时，需要书面申请并取得授权后，由专人全程陪同并登记备案；访问受控网络时需书面申请，开设访客账户，分配权限，登记备案；离场后及时清除来访者权限；与外部授权人员签保密协议，不得复制和泄露敏感信息；核心关键区域及应用原则不允许外部人员访问。

系统安全建设包括依据备案等级选择安全措施，根据风险调整防范措施，对网络系统进行安全整体规划和方案设计并形成配套文件，完成对安全整体规划及配套文件的评审，并开始实施。在系统实施阶段需要选择符合国家规定网络安全产品和符合密码主管部门有关规定的密码产品，重要部位产品需委托专项测试后再进行选择。在自主软件方面，需实际开发与实际环境分离，软件代码编写规范，开发过程文档完备，程序资源库的修改、更新、发布进行严格授权，严格版本控制，开发活动需要进行受控并进行恶意代码检测。在外采软件方面需进行恶意代码检测，并要求其提供完备的文档与使用指南。在工程实施时需由专人管理实施过程并制定工程实施方案。有条件的报业集团需要实行第三方监理。在系统验收阶段，要求具有验收方案，验收报告，上线前安全测试报告，包含密码应用的安全性等测试。在系统交付时，需要提供交付清单、人员培训、建设过程文档和运维文档。

系统安全运维管理包括了机房环境管理、资产管理、运行监控、数据备份、安全措施的落实等，需要专人负责机房安全管理。机房环境的管理包括：机房进出与运维管理、机房安全管理制度，含敏感信息介质和文档不随意放置，对出入人员按级别授权，重要区域实时监控；资产管理包括：资产清单、资产标识管理及资产管理人员；机房介质管理包括：安全存放，专用介质专人管理，定期盘点，介质流转控制并记录；漏洞与风险管理包括：检查、及时修补或评估后修补，风险测评并形成报告及采取措施应对。制定重要设备配置与操作手册，记录运维日志，分析日志与监控数据；操作中保留日志，同步更新配置库；严格运维工具使用，保留日志，及时删除敏感信息；恶意代码防范管理包括外来接入要先查杀病毒、规定恶意代码防范要求、检查病毒库升级，并分析捕获样本，定期验证防病毒技术措施的有效性；备份与恢复管理包括识别需备份的重要业务信息、系统数据与软件，规定备份方式、介质、频率等，制定备份策略和恢复策略和程序；安全事件处置包括及时报告安全事件、制定安全事件报告与处置管理制度，分析原因，总结教训，对重大服务中断与信息泄露事件有不同的处理流程与报告程序，建立联合防护和应急机制，处置跨单位安全事件。

3. 日常管理问题与思考

信息安全系统从信息安全管理、信息安全技术和信息安全运行三个方面进行了全面的约定，通过这三方面的建设形成了一套完备的信息安全体系，在落实到位的情况下，完全符合等级保护测评的各项指标。然后，在实际工作中很多报业集团安全体系往往流于形式，执行不到位，只是用于等级保护测评。导致这种情况发生的原因主要是对网络系统的安全防护意识不够，费用预算不足，人员配备不到位，从而导致安全策略执行不到位，安全制度形同虚设。有的虽然网络安全等级测评合格了，但网络系统安全的隐患还很大，只有严格按照既定的要求进行日常管理，才能保障测评合格的网络系统安全运行。媒

参考文献

[1] 林宁思，赖建华．电子政务网站群安全防护体系研究 [J]. 福建电脑，2011-08-25.

[2] 许程亮．电子招标投标系统安全风险分析及应对措施 [J]. 招标采购管理，2017-10-25.

（作者单位：河北日报报业集团）